A list of information security related awesome lists and other resources.

GoVanguard InfoSec Encyclopedia

This is an ongoing compilation of resources we have found helpful and tools we use.If you're new to InfoSec and are looking for a concentrated list of resources to get started, check out Getting into InfoSec and Cybersecurity.

Table of Contents

- Resources
  - Information Security Certifications
  - Books
  - Lockpicking Resources
  - Social Engineering Articles
  - Conferences
  - Online Videos
  - Free Online Courses
  - Training Resources
  - Hacking References And Cheatsheets
  - Training And Practice Exercises
  - Informative Youtube Channels
  - Illustrations and Presentations
  - Clearnet Exploit Databases
  - Awesome Master Lists
  - Knowledge Bases
- OSINT Tools Used
  - General OSINT Tools
  - Crypto OSINT Search
  - Government Record Search
  - National Search Engines
  - Meta Search
  - Visual Search and Clustering Search Engines
  - Similar Sites Search
  - Document and Slides Search
  - Pastebin Search
  - Code Search
  - Real-Time Search, Social Media Search, and General Social Media Tools
  - Twitter Search
  - Facebook Search
  - Instagram Search
  - Pinterest Search
  - Reddit Search
  - VKontakte Search
  - LinkedIn
  - Blog Search
  - Forums and Discussion Boards Search
  - Username Check
  - Personel Investigations

    - E-mail Search / E-mail Check
    - Phone Number Research
    - Company Research
    - Domain and IP Research
    - Keywords Discovery and Research
    - Web History and Website Capture
    - Language Tools
    - Image Search
    - Image Analysis
    - Data and Statistics
    - Web Monitoring
    - OCR Tools
    - Collaboration and Project Management
    - Communication Tools
    - Calendars and Scheduling
    - Mind Mapping, Concept Mapping and Idea Generation Tools
    - Social Network Analysis
    - DNS Search And Enumeration
    - Network Reconnaissance Tools
- Exploitation Enumeration And Data Recovery Tools
    - Penetration Testing OS Distributions
    - Multi-paradigm Frameworks
    - Network Vulnerability Scanners
    - Web Vulnerability Scanners
    - Web Exploitation
    - Network Tools
    - Protocol Analyzers and Sniffers
    - Proxies and MITM Tools
    - Wireless Network Tools
    - Transport Layer Security Tools
    - Cryptography
    - Post-Exploitation
    - Exfiltration Tools
    - Static Analyzers
    - Dynamic Analyzers
    - Hex Editors
    - File Format Analysis Tools
    - Anti-Virus Evasion Tools
    - Hash Cracking Tools
    - Windows Utilities
    - GNU Linux Utilities
    - macOS Utilities
    - Social Engineering Tools
    - Anonymity Tools
    - Reverse Engineering Tools
    - Side-channel Tools
    - Forensic Tools
    - Memory Analysis
    - Memory Imaging Tools
    - Incident Response
    - Honeypot Tools
    - Monitoring and IDS-IPS

    - Physical Tools
    - Adversary Emulation
    - All in one Incident Response Tools
    - Communities
    - Disk Image Creation Tools
    - Evidence Collection Tools
    - Incident Management Tools
    - Linux Forensics Distributions
    - Linux Evidence Collection
    - Log Analysis Tools
    - OSX Evidence Collection
    - Incident Response Playbooks
    - Process Dump Tools
    - Sandboxing/reversing tools
    - Timeline tools
    - Windows Evidence Collection
    - Other
- License

Resources

Information Security Certifications

- Certified Ethical Hacker
- Certified Information Systems Security Professional (CISSP)
- Certified Penetration Testing Engineer (CPTE)
- CompTIA Security+
- GIAC Security Essentials (GSEC)
- Kali Linux Certified Professional (KLCP)
- Offensive Security Certified Expert (OSCE)
- Offensive Security Certified Professional (OSCP)
- Offensive Security Exploitation Expert (OSEE)
- Offensive Security Web Expert (OSWE)
- Offensive Security Wireless Professional (OSWP)

Books

- A Bug Hunter's Diary: A Guided Tour Through the Wilds of Software Security
- A Short Course on Computer Viruses
- AVIEN Malware Defense Guide for the Enterprise
- Advanced Penetration Testing: Hacking the World's Most Secure Networks
- Applied Cryptography: Protocols, Algorithms and Source Code in C
- Applied Network Security Monitoring: Collection, Detection, and Analysis
- Black Hat Python: Python Programming for Hackers and Pentesters
- Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder
- Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications
- CEH Certified Ethical Hacker All-in-One Exam Guide
- CISSP All-in-One Exam Guide

- CISSP: Certified Information Systems Security Professional Study Guide
- CISSP](ISC)2 Certified Information Systems Security Professional Official Study Guide
- Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon
- Cryptography Engineering: Design Principles and Practical Applications
- Cyber War: The Next Threat to National Security and What to Do About It
- Cybersecurity - Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare
- Cybersecurity and Cyberwar: What Everyone Needs to Know
- Cybersecurity and Human Rights in the Age of Cyberveillance
- Cyberspies: The Secret History of Surveillance, Hacking, and Digital Espionage
- Essentials of Cybersecurity
- Future Crimes: Inside the Digital Underground and the Battle for Our Connected World
- Ghost in the Wires: My Adventures as the World's Most Wanted Hacker
- Hacked Again
- Hacking Exposed 7
- Hacking: The Art of Exploitation
- How Linux Works: What every superuser should know
- Information Assurance Handbook: Effective Computer Security and Risk Management Strategies
- Linux Shell Scripting Cookbook
- Network Forensics: Tracking Hackers through Cyberspace
- Network Security Through Data Analysis: Building Situational Awareness
- Penetration Testing: A Hands-On Introduction to Hacking
- Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software
- Practice of Network Security Monitoring
- Protecting Your Internet Identity: Are You Naked Online?
- Protection and Security on the Information Superhighway
- Reversing: Secrets of Reverse Engineering
- Rtfm: Red Team Field Manual
- Security Metrics, A Beginner's Guide
- Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door
- Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection
- TCP/IP Illustrated
- The Art of Computer Virus Research and Defense
- The Art of Deception: Controlling the Human Element of Security
- The Art of Memory Forensics
- The Beginner's Guide to Information Security
- The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography
- The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk
- The Cyber Skill Gap
- The Hacker Playbook: Practical Guide To Penetration Testing
- The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler
- The Ncsa Guide to PC and Lan Security
- The Shellcoder's Handbook: Discovering and Exploiting Security Holes
- The Tao of Network Security Monitoring: Beyond Intrusion Detection

- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws
- Thinking Security: Stopping Next Year's Hackers
- Understanding Cryptography: A Textbook for Students and Practitioners
- We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency
- Web Application Vulnerabilities: Detect, Exploit, Prevent
- Windows Internals
- Worm: The First Digital World War
- A Search Engine Backed by Internet-Wide Scanning - Ariana Mirian
- Advanced Penetration Testing by Wil Allsopp, 2017
- Advanced Penetration Testing for Highly-Secured Environments by Lee Allen, 2012
- Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization by Tyler Wrightson, 2014
- Android Hackers Handbook by Joshua J. Drake et al., 2014
- Black Hat Python: Python Programming for Hackers and Pentesters by Justin Seitz, 2014
- Btfm: Blue Team Field Manual by Alan White and Ben Clark
- Bug Hunter's Diary by Tobias Klein, 2011
- CIA Lock Picking Field Operative Training Manual
- Car Hacker's Handbook by Craig Smith, 2016
- CompTIA Security+ SY0-501 Certification Study Guide
- Complete Guide to Shodan
- Dfir intro
- Eddie the Wire books
- Essentials of Enterprise Network Security
- Fuzzing: Brute Force Vulnerability Discovery by Michael Sutton et al., 2007
- Ghost in the Wires by Kevin D. Mitnick & William L. Simon, 2011
- Gray Hat Hacking The Ethical Hacker's Handbook by Daniel Regalado et al., 2015
- Hacking the Xbox by Andrew Huang, 2003
- Holistic Info-Sec for Web Developers](https://leanpub.com/b/holisticinfosecforwebdevelopers)
- Kali Linux Revealed
- Keys to the Kingdom by Deviant Ollam, 2012
- Lock Picking: Detail Overkill by Solomon
- Malware Analyst's Cookbook and DVD by Michael Hale Ligh et al., 2010
- Metasploit: The Penetration Tester's Guide by David Kennedy et al., 2011
- Network Forensics: Tracking Hackers through Cyberspace by Sherri Davidoff & Jonathan Ham, 2012
- Network Security Assessment by Chris McNab
- Nmap Network Scanning by Gordon Fyodor Lyon, 2009
- No Tech Hacking by Johnny Long & Jack Wiles, 2008
- Open Source Intelligence Techniques - 8th Edition by Michael Bazell, 2021
- Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman, 2014
- Penetration Testing: Procedures & Methodologies by EC-Council, 2010
- Practical Lock Picking by Deviant Ollam, 2012
- Practical Malware Analysis by Michael Sikorski & Andrew Honig, 2012
- Practical Packet Analysis by Chris Sanders, 2017
- Practical Reverse Engineering by Bruce Dang et al., 2014
- Professional Penetration Testing by Thomas Wilhelm, 2013
- Reverse Engineering for Beginners by Dennis Yurichev

- Rtfm: Red Team Field Manual by Ben Clark, 2014
- Secure Programming HOWTO
- Social Engineering in IT Security: Tools, Tactics, and Techniques by Sharon Conheady, 2014
- Social Engineering: The Art of Human Hacking by Christopher Hadnagy, 2010
- The Art of Deception by Kevin D. Mitnick & William L. Simon, 2002
- The Art of Exploitation by Jon Erickson, 2008
- The Art of Intrusion by Kevin D. Mitnick & William L. Simon, 2005
- The Art of Memory Forensics by Michael Hale Ligh et al., 2014
- The Basics of Hacking and Penetration Testing by Patrick Engebretson, 2013
- The Browser Hackers Handbook by Wade Alcorn et al., 2014
- The Database Hacker's Handbook, David Litchfield et al., 2005
- The Hacker Playbook by Peter Kim, 2014
- The IDA Pro Book by Chris Eagle, 2011
- The Mac Hacker's Handbook by Charlie Miller & Dino Dai Zovi, 2009
- The Mobile Application Hackers Handbook by Dominic Chell et al., 2015
- The Practice of Network Security Monitoring: Understanding Incident Detection and Response 9
- The Shellcoders Handbook by Chris Anley et al., 2007
- The Web Application Hackers Handbook by D. Stuttard, M. Pinto, 2011
- Unauthorised Access: Physical Penetration Testing For IT Security Teams by Wil Allsopp, 2010
- Unmasking the Social Engineer: The Human Element of Security by Christopher Hadnagy, 2014
- Violent Python by TJ O'Connor, 2012
- Windows Internals by Mark Russinovich et al., 2012
- Wireshark Network Analysis by Laura Chappell & Gerald Combs, 2012
- iOS Hackers Handbook by Charlie Miller et al., 2012

Lockpicking Resources

- /r/lockpicking Subreddit - Subreddit dedicated to the sport of lockpicking.
- Keypicking.com - Bustling online forum for the discussion of lockpicking and locksport.
- LockWiki - Community-driven reference for both beginners and professionals in the security industry.
- Lockpicking Forensics - Website "dedicated to the science and study of forensic locksmithing."
- Lockpicking101.com - One of the longest-running online communities "dedicated to the fun and ethical hobby of lock picking."
- The Amazing King's Lockpicking pages - Hobbyist's website with detailed pages about locks, tools, and picking techniques.

Social Engineering Articles

- How I Socially Engineer Myself Into High Security Facilities - Sophie Daniel
- Social Engineering: Compromising Users with an Office Document - Infosec Institute
- The 7 Best Social Engineering Attacks Ever - DarkReading
- The Limits of Social Engineering - MIT, Technology Review
- The Persuasion Reading List - Scott Adams' Blog

Conferences

- (ISC)2 Secure Event Series
- 44CON London
- 44Con
- AFCEA Defensive Cyber Operations Symposium
- AppSec United States](OWASP National Conference)
- AppSecUSA
- Atlantic Security Conference](AtlSecCon)
- BSides
- BSides Event Series
- BalCCon
- Black Hat
- Black Hat United States
- BruCON
- CCC
- CISO Executive Summit Series](Invite-only)
- CSO50 Conference
- CanSecWest
- CarolinaCon
- Cyber Threat Intelligence Summit
- DEF CON
- DeepSec
- DefCamp
- DerbyCon
- DerbyCon 8.0
- Ekoparty
- FIRST Conference
- FSec
- HACKMIAMI
- HITB
- HOPE
- Hack.lu
- Hack3rCon
- Hacker Halted - Optionally includes certification-specific training
- IANS Information Security Forums
- IAPP Global Privacy Summit
- IEEE Symposium on Security & Privacy
- ISACA Cyber Security Nexus
- ISF Annual World Congress
- ISSA CISO Executive Forum Series
- ISSA International Conference
- Ignite
- Infiltrate
- InfoSec Southwest
- InfoSec World
- Infosecurity Europe
- Infosecurity Europe
- Infosecurity North America
- LayerOne
- Nullcon
- Nullcon Conference
- Open Security Summit
- PhreakNIC

- RSA Conference United States
- SANS Annual Conference
- SANS Pen Test Annual Conferences
- SANS Security Annual Conferences
- SECUINSIDE
- SOURCE Annual Conferences
- SecTor Canada
- Secure360 Conference
- SecureWorld
- Securi-Tay
- Security Operations Summit & Training
- ShmooCon
- SkyDogCon
- SummerCon
- Swiss Cyber Storm
- ThotCon
- USENIX Security Symposium
- Virus Bulletin Conference
- conINT
- secureCISO

Online Videos

- Dennis Maldonado: Are We Really Safe? Bypassing Access Control Systems
- Internet of Things: IoT Research Methodology
- Internet of Things: The Relationship Between IoT and Security
- Offensive Security Part 1 - Basics of Penetration Testing
- Phishing Campaigns in Metasploit Pro
- Rapid7 Whiteboard Wednesday Series
- Spear Phishing with Cobalt Strike

Free Online Courses

- CompTIA Network+ Certification Video Course By PowerCert Animated Videos
- CompTIA Security+ SY0-501 Training Course By Professor Messer
- Complete Ethical Hacking Course By HackerSploit - Part1 of 126
- Complete Ethical Hacking Course by Joseph Delgadillo - 8 hour course

Training Resources

- Awesome Hacking Resources - Self-explanatory.
- Awesome Web Security - Encyclopedia of web security information.
- Corelan.be - Website containing many useful training resources and tutorial.
- Cybrary.it - Free online courses.
- Enigma Group - Web application training resource.
- Executing Metasploit & Empire Payloads from MS Office Document Properties part 1 - How to stealthily deliver a Metasploit payload via MS Office document properties and a simple macro.
- Executing Metasploit & Empire Payloads from MS Office Document Properties part 2 - Like part 1, but focusing on Empire rather than Metasploit.
- Hacker101 - Online training resource.
- How To: Empire's Cross Platform Office Macro - How to utilize Empire's cross-platform malicious MS Office macro.

- Introduction to Software Exploits Part 1 - Online or in-person tutorial covering multiple areas of software exploitation.
- Introduction to Software Exploits Part 2 - Exploitation in the Windows Environment - Online or in-person tutorial covering multiple areas of software exploitation, with emphasis on Windows exploitation.
- OpenSecurityTraining.info - Free online training resource.
- PentesterLab - Tiered online training resources.
- Phishing With Empire - Guide on phishing with Empire.
- Phishing With PowerPoint - Guide on getting unsuspecting users to open malicious PPT files.

Hacking References And Cheatsheets

- LFI Cheat Sheet
- Local Linux Enumeration & Privilege Escalation Cheatsheet
- Metasploit Payload Cheatsheet
- Multiple Cheatsheets By Andrewjkerr
- Nmap Cheat Sheet
- Pentest Recon And Enu Cheatsheet
- Reverse Shell Cheat Sheet
- SQL Injection Cheat Sheet
- XSS Cheat Sheet
- XSS Payload Cheatsheet

Training And Practice Exercises

- CPTE Courseware Kit - Paid Official training kit for CPTE exam.
- Damn Vulnerable Web Application (DVWA) - Purposely vulnerable PHP/MySQL web application.
- Gruyere - Gruyere is a web application that has multiple security bugs ranging from cross-site scripting and cross-site request forgery, to information disclosure, denial of service, and remote code execution.
- Hack This Site - Web application security exercises.
- Hack the Box - Online pentesting labs with Windows VMs.
- Hacker101 CTF - Webapp CTF style exercises.
- Mutillidae - Mutillidae is a free, open source web application provided to allow you to hack a web application. Can be installed on Linux, Windows XP, Windows 7 and windows 10 using XAMMP.
- OSCP-like Vulnhub VMs - Intentionally vulnerable VMs resembling OSCP.
- OWASP Damn Vulnerable Web Sockets (DVWS) - Vulnerable web application which works on web sockets for client-server communication.
- OWASP Juice Shop - JavaScript based intentionally insecure web application.
- OWASP NodeGoat - Includes Node.js web applications for learning the OWASP top 10.
- OWASP Railsgoat - A vulnerable version of Rails that follows the OWASP Top 10.
- OWASP SecurityShepard - Web and mobile application security training platform.
- OWASP WebGoat - WebGoat is an insecure application that allows the testing of vulnerabilities commonly found in Java-based applications that use common and popular open source components.
- OWASP security knowledge framework - OWASP security knowledge framework labs exercises complete with write-ups.
- Over the Wire: Natas - Web application challenges.

- Rapid7 Metsploitable - Metasploitable is essentially a penetration testing lab in a box, available as a VMware virtual machine (VMX).
- RopeyTasks - Simple deliberately vulnerable web application.
- XSS Exercises - Webapp Cross-site scripting (XSS) bug hunting exercises.

Informative Youtube Channels

- Computerphile - Information security concepts.
- Hacksplained - Hacking guides and walkthroughs.
- Hak5 - Hacking tools, guides and concepts.
- Loi Liang Yang - Hacking guides.
- Motasem Hamdan - Hacking guides.
- Null Byte - Hacking guides and concepts.
- Schuyler Towne channel - Lockpicking videos and security talks.
- Thenewboston - Programming and hacking guides.
- bosnianbill - lockpicking videos.

Illustrations and Presentations

- "Fileless" UAC Bypass Using sdclt.exe
- A Citrix Story
- A Guide to Attacking Domain Trusts
- A Guide to Attacking Domain Trusts
- A Pentester's Guide to Group Scoping
- A Read Teamer's Guide to GPOs and OUs
- Abusing Active Directory Permissions with PowerView
- Abusing DCOM For Yet Another Lateral Movement Technique
- Abusing DNSAdmins Privilege for Escalation in Active Directory
- Abusing Exported Functions and Exposed DCOM Interfaces for Pass-Thru Command Execution and Lateral Movement
- Abusing GPO Permissions
- Abusing Microsoft Word Features for Phishing: "subDoc"
- Abusing the COM Registry Structure: CLSID, LocalServer32, & ImprocServer32
- Accessing Clipboard From the Lock Screen in Windows 10 Part 1
- Accessing Clipboard From the Lock Screen in Windows 10 Part 2
- Agentless Post-Exploitation
- Aggressor PowerView
- AppLocker - Case Study - How Insecure Is It Really? Part 1
- AppLocker - Case Study - How Insecure Is It Really? Part 2
- Are We Really Safe? Hacking Access Control Systems
- Automated Derivative Administrator Search
- Awesome Bug Bounty
- Awesome CTF
- Awesome ICS Security
- Awesome Lockpicking
- Awesome Yara
- Bringing the Hashes Home With reGeorg & Empire
- Bypassing AMSI via COM Server Hijacking
- Bypassing Application Whitelisting With BGinfo
- Bypassing Device Guard UMCI Using CHM - CVE-2017-8625
- Bypassing UAC Using App Paths
- Cell Injection

- ClickOnce, Twice or Thrice: A Technique for Social Engineering and Untrusted Command Execution
- Cloning and Hosting Evil Captive Portals Using a Wi-Fi Pineapple
- CloudFront Hijacking
- Cobalt Strike - What's the go-to phishing technique or exploit?
- Code Signing Certificate Cloning Attacks and Defenses
- Colbalt Strike - Spear Phishing documentation
- Comma Separated Vulnerabilities
- DNS Data Exfiltration - What is This and How to Use?
- DNS Tunnelling
- Data Exfiltration Over DNS Request Covert Channel: DNSExfiltrator
- Data Exfiltration via Formula Injection
- Defense In Depth
- DiskShadow: The Return of VSS Evasion, Persistence, and Active Directory Database Extraction
- Domain Fronting Via Cloudfront Alternate Domains
- Dump Clear-Text Passwords for All Admins in the Domain Using Mimikatz DCSync
- Dumping Domain Password Hashes
- Empire Domain Fronting
- Empire Without PowerShell
- Escape and Evasion Egressing Restricted Networks
- Excel Macros With PowerShell
- Executing Commands and Bypassing AppLocker with PowerShell Diagnostic Scripts
- Exploiting Environment Variables in Scheduled Tasks for UAC Bypass
- Extending BloodHound for Red Teamers
- Finding Domain Frontable Azure Domains
- First Entry: Welcome and Fileless UAC Bypass
- From Pass-the-Hash to Pass-the-Ticket with No Pain
- Getting the Goods with CrackMapExec: Part 1
- Getting the Goods with CrackMapExec: Part 2
- Harden Windows With AppLocker - Based on Case Study Part 1
- Harden Windows With AppLocker - Based on Case Study Part 2
- Hiding Registry Keys with PSReflect
- How I Identified 93k Domain-Frontable CloudFront Domains
- How to Obfuscate JacaScript in Metasploit
- In-Memory Evasion
- Intercepting Passwords With Empire and Winning
- Intro to Using GScript for Red Teams
- Introducing BloodHound
- Introduction to Metasploit: Exploiting Web Applications
- Jumping Network Segregation with RDP
- Kerberoasting Without Mimikatz
- Kerberos Party Tricks: Weaponizing Kerberos Protocol Flaws
- Lateral Movement Using Excel Application and docm
- Lay of the Land with Bloodhound
- LethalHTA - A New Lateral Movement Technique Using DCOM and HTA
- Leveraging INF-SCT Fetch & Execute Technique For Bypass, Evasion, & Persistence
- Leveraging INF-SCT Fetch & Execute Technique For Bypass, Evasion, & Persistence
- Loading Alternate Data Stream ADS DLL/CPL Binaries to Bypass AppLocker

- Local Administrator Password Solution (LAPS) - Part 1
- Local Administrator Password Solution (LAPS) - Part 2
- Local Group Enumeration
- Macro-less Code Exec in MSWord
- Microsoft LAPS Security & Active Directory LAPS Configuration Recon
- Microsoft Office - NTLM Hashes via Frameset
- Multi-Platform Macro Phishing Payloads
- My First Go with BloodHound
- OPSEC Considerations for Beacon Commands
- OWASP Social Engineering: The Art of Human Hacking
- Offensive Encrypted Data Storage
- Office 365 Safe Links Bypass
- Outlook Forms and Shells
- Outlook Home Page - Another Ruler Vector
- Pass-the-Hash is Dead: Long Live LocalAccountTokenFilterPolicy
- Persistence Using Globalflags In Image File Execution Options - Hidden from Autoruns.exe
- Persistence Using RunOnceEx - Hidden from Autoruns.exe
- Phishing Against Protected View
- PowerPoint and Custom Actions
- PowerShell Empire Stagers 1: Phishing With an Office Macro and Evading AVs
- PowerShell Without PowerShell - How To Bypass Application Whitelisting, Environment Restrictions & AV
- Practical Guide to NTLM Relaying in 2017
- Process Doppleganging - A New Way to Impersonate A Process
- Putting Data In Alternate Data Streams and How to Execute It
- Putting Data in Alternate Data Streams and How to Execute It
- Red Team Insights on HTTPS Domain Fronting Google Hosts Using Cobalt Strike
- Red Team Operating in a Modern Environment
- Roasting AS-REPs
- SPN Discovery
- Scanning for Active Directory Privileges & Privileged Accounts
- Simple Domain Fronting PoC with GAE C2 Server
- Spear Phishing 101
- Targeted Kerberoasting
- The Absurdly Underestimated Dangers of CSV Injection
- The Most Dangerous User Right You Probably Have Never Heard Of
- The PowerView PowerUsage Series #1 - Mass User Profile Enumeration
- The PowerView PowerUsage Series #2 - Mapping Computer Shortnames With the Global Catalog
- The PowerView PowerUsage Series #3 - Enumerating GPO Edit Rights In a Foreign Domain
- The PowerView PowerUsage Series #4 - Finding Cross-Trust ACEs
- Trust Direction: An Enabler for Active Directory Enumeration and Trust Exploitation
- Ultimate AppLocker ByPass List
- Userland API Monitoring and Code Injection Detection
- Using SQL Server for Attacking a Forest Trust
- Using a SCF File to Gather Hashes
- Using robots.txt to Locate Your Targets
- Validated CloudFront SSL Domains

- Vshadow: Abusing the Volume Shadow Service for Evasion, Persistence, and Active Directory Database Extraction
- WMI Persistence with Cobalt Strike
- WSH Injection: A Case Study
- Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter
- Week of Evading Microsoft ATA
- Windows Access Tokens and Alternate Credentials
- Windows Defender Attack Surface Reduction Rules Bypass
- Windows Oneliners to Download Remote Payload and Execute Arbitrary Code
- Windows Privilege Escalation checklist
- android-security-awesome
- harmj0y Presentations and Blogs - Windows and Active Directory Exploitation
- mavinject.exe Functionality Deconstructed
- sg1: swiss army knife for data encryption, exfiltration & covert communication

Clearnet Exploit Databases

- 0day.today
- Awesome CVE PoC
- Contagio
- Exploit-DB
- InfoSec - CERT-PA
- MalShare
- Packet Storm Security
- Tracker h3x
- VX Vault
- VirusBay
- VirusShare
- VirusSign
- Zeus Trojan source code
- theZoo

Awesome Master Lists

- Also Hacking
- Android Security Analysis
- Application Security
- Bug Bounty
- CVE Proof of Concepts
- Capture The Flag
- Exploit Development
- Forensics
- Hacking Lists
- Hacking Resources
- Hacking
- Honeypot
- Incident Response
- Industrial Control System Security
- Lockpicking
- Malware Analysis
- OSINT
- Packet Capture Tools

- PenTesting
- Penetration Testing - Supported by Netsparker
- Red Teaming
- SecLists - Useful security related lists to reference/work off of in a pentest
- Security Talks
- Security
- Starting Up Security - A collection of information security essays and links to help growing teams manage risks.
- Threat Intelligence
- Web Security
- YARA

Knowledge Bases

- 0day
- Alienvault Open Threat Exchange (OTX) - Live threat feed.
- Cvedetails
- CyBOK
- Exploit-db
- Jetlib
- MITRE ATT&CK
- Mitre
- Nvd.nist.gov
- OSINT Intel Techniques
- Openwall
- Packetstormsecurity
- Rapid7
- Securityfocus
- Seebug
- Talos Intelligence - Live threat feed.
- Top 100 Cyber Security Blogs and Websites
- Vulnerability-lab
- Wpvulndb
- Zerodayinitiative

OSINT Tools Used

General OSINT Tools

- AbuseIPDB - Search engine for blacklisted IPs or domains.
- AutoShun - Public repository of malicious IPs and other resources.
- BadIPs - Online blacklist lookup.
- Barcode Reader - Decode barcodes in C#, VB, Java, C\C++, Delphi, PHP and other languages.
- Belati - The Traditional Swiss Army Knife For OSINT. Belati is tool for Collecting Public Data & Public Document from Website and other service for OSINT purpose.
- Binary Defense IP Ban List - Public IP blacklist.
- Blocklist Ipsets - Public IP blacklist.
- Censys - Collects data on hosts and websites through daily ZMap and ZGrab scans.
- CloudFrunt - Tool for identifying misconfigured CloudFront domains.

- Combine - Open source threat intelligence feed gathering tool.
- Creepy - Geolocation OSINT tool.
- Datasploit - Tool to perform various OSINT techniques on usernames, emails addresses, and domains.
- Dnsenum - Perl script that enumerates DNS information from a domain, attempts zone transfers, performs a brute force dictionary style attack, and then performs reverse look-ups on the results.
- Dnsmap - Passive DNS network mapper.
- Dnsrecon - DNS enumeration script.
- Dnstracer - Determines where a given DNS server gets its information from, and follows the chain of DNS servers.
- Dork-cli - Command line Google dork tool.
- emagnet - Automated hacking tool that will find leaked databases.
- FindFrontableDomains - Multithreaded tool for finding frontable domains.
- GOSINT - OSINT tool with multiple modules and a telegram scraper.
- Github-dorks - CLI tool to scan github repos/organizations for potential sensitive information leak.
- GooDork - Command line Google dorking tool.
- Google Hacking Database - Database of Google dorks; can be used for recon.
- Greynoise - "Anti-Threat Intelligence" Greynoise characterizes the background noise of the internet, so the user can focus on what is actually important.
- InfoByIp - Domain and IP bulk lookup tool.
- Intrigue Core - Framework for attack surface discovery.
- Machinae - Multipurpose OSINT tool using threat intelligence feeds.
- Maltego - Proprietary software for open source intelligence and forensics, from Paterva.
- Malware Domain List - Search and share malicious URLs.
- NetBootcamp OSINT Tools
- OSINT Framework
- OpenRefine - Free & open source power tool for working with messy data and improving it.
- Orbit - Draws relationships between crypto wallets with recursive crawling of transaction history.
- OsintStalker - Python script for Facebook and geolocation OSINT.
- Outwit - Find, grab and organize all kinds of data and media from online sources.
- PaGoDo - Passive, automated Google dorking tool.
- Passivedns-client - Library and query tool for querying several passive DNS providers.
- Passivedns - Network sniffer that logs all DNS server replies for use in a passive DNS setup.
- Photon - Crawler designed for OSINT.
- Pown Recon - Target reconnaissance framework powered by graph theory.
- QuickCode - Python and R data analysis environment.
- Raven - LinkedIn information gathering tool.
- Recon-ng - Full-featured Web Reconnaissance framework written in Python.
- SecApps Recon - Information gathering and target reconnaissance tool and UI.
- Spamcop - IP based blacklist.
- Spamhaus - Online blacklist lookup.
- Spiderfoot - Open source OSINT automation tool with a Web UI and report visualizations
- ThreatCrowd - Threat search engine.
- ThreatTracker - Python based IOC tracker.

- Vcsmap - Plugin-based tool to scan public version control systems for sensitive information.
- XRay - XRay is a tool for recon, mapping and OSINT gathering from public networks.
- Zen - Find email addresses of Github users.
- malc0de DNSSinkhole - List of domains that have been identified as distributing malware during the past 30 days.
- malc0de Database - Searchable incident database.
- pygreynoise - Greynoise Python Library
- sn0int - Semi-automatic OSINT framework and package manager.
- theHarvester - E-mail, subdomain and people names harvester.

Crypto OSINT Search

- Bitcoin Abuse - Database of wallets associated with ransomware, blackmailers and fraud.
- Bitcoin Who's Who - Database of known ID information from bitcoin addresses.
- Blockchair - Multiple blockchain explorer.
- Wallet Explorer - Finds all known associated bitcoin addresses from a single known address.

Government Record Search

- Blackbook - Public Records Starting Point.
- FOIA Search - Government information request portal.
- PACER - Public Access to Federal Court Records.
- RECAP - Free version of PACER. Includes browser extensions for Chrome & Firefox.
- SSN Validator - Confirms valid Social Security Numbers.

National Search Engines

Localized search engines by country.

- Alleba (Philippines)
- Baidu (China)
- Eniro (Sweden)
- Goo (Japan)
- Najdsi (Slovenia)
- Naver (South Korea)
- Onet.pl (Poland)
- Orange (France)
- Parseek (Iran)
- SAPO (Portugal)
- Search.ch (Switzerland)
- Walla (Israel)
- Yandex (Russia)

Meta Search

Lesser known and used search engines.

- All-in-One
- AllTheInternet

- Etools
- FaganFinder
- Goofram
- Myallsearch
- Qwant
- Sputtr
- Trovando
- WebOasis
- Zapmeta
- iZito

Visual Search and Clustering Search Engines

Search engines that scrape multiple sites (Google, Yahoo, Bing, Goo, etc) at the same time and return results.

- Carrot2 * Organizes your search results into topics.
- Yippy * Search using multiple sources at once

Document and Slides Search

Search for data located on PDFs, Word documents, presentation slides, and more.

- Authorstream
- Find-pdf-doc
- Free Full PDF
- Offshore Leak Database
- PDF Search Engine
- RECAP
- Scribd
- SlideShare
- Slideworld
- soPDF.com

Pastebin Search

- Pastebin - Pastebin is a website where you can store any text online for easy sharing.

Code Search

Search by website source code

- NerdyData - Search engine for source code.
- SearchCode - Help find real world examples of functions, API's and libraries across 10+ sources.

Real-Time Search, Social Media Search, and General Social Media Tools

- Audiense
- Blazent
- Brandwatch
- Buffer

- Buzz sumo
- Geocreepy
- Geofeedia
- Hootsuite
- Hashtatit
- Klear
- Kred
- SproutSocial
- Netvibes
- OpinionCrawl
- Rival IQ
- RSS Social Analyzer
- SocialBakers
- SociaBlade
- Social DownORNot
- Social Searcher
- Tagboard
- Reputation Refinery
- UVRX

Twitter Search

- Backtweets
- Fake Follower Check
- First Tweet
- FirstTweet
- Foller.me
- FollowCheck
- Followerwonk
- GeoSocial Footprint
- Geochirp
- Gigatweeter
- Ground Signal
- HappyGrumpy
- Harvard TweetMap
- Hashtagify
- Hashtags.org
- ManageFlitter
- Mentionmapp
- OneMillionTweetMap
- Rank Speed
- Riffle
- RiteTag
- Schedule Warble
- Sentiment140
- Sleeping Time
- Social Bearing
- TruFan
- Spoonbill
- TWUBS Twitter Chat
- Tagdef
- Tinfoleak
- Trends24

- TrendsMap
- TwChat
- Twazzup
- Tweet Tag
- TweetArchivist
- TweetDeck
- TweetMap
- TweetMap
- TweetPsych
- TweetStats
- TweetTunnel
- Tweetreach
- Twellow
- Tweriod
- Twiangulate
- Twicsy
- Twilert
- Twipho
- TwitRSS
- Twitonomy
- Twitter Advanced Search
- Twitter Audit
- Twitter Chat Schedule
- Twitter Search
- Twitterfall
- burrrd.
- doesfollow

Facebook Search

- Agora Pulse
- Commun.it
- ExtractFace
- Fanpage Karma
- Facebook Search
- Facebook Search Tool
- FaceLIVE
- Fb-sleep-stats
- Find my Facebook ID
- Lookup-ID.com
- SearchIsBack
- Wallfux
- Wolfram Alpha Facebook Report
- Zesty Facebook Search

Instagram Search

- Hashtagify
- Iconosquare
- Picodash
- SnapMap
- Social Rank
- Worldcam

Pinterest Search

- Pingroupie

Reddit Search

Tools to help discover more about a reddit user or subreddit.

- Imgur - The most popular image hosting website used by redditors.
- Mostly Harmless - Mostly Harmless looks up the page you are currently viewing to see if it has been submitted to reddit.
- Reddit Archive - Historical archives of reddit posts.
- Reddit Comment Search - Analyze a reddit users by comment history.
- Reddit Investigator - Investigate a reddit users history.
- Reddit Suite - Enhances your reddit experience.
- Reddit User Analyser - reddit user account analyzer.
- Subreddits - Discover new subreddits.

VKontakte Search

Perform various OSINT on Russian social media site VKontakte.

- Barkov.net
- Report Tree
- Snradar - Search pictures by time and location they were taken
- Social Stats
- Target Hunter
- Target Log
- VK Community Search
- VK Parser - A tool to search for a target audience and potential customers.
- VK People Search
- VK to RSS Appspot
- VK5
- Дезертир

Blog Search

- BlogSearchEngine
- Notey - Blog post search engine.
- Outbrain
- Twingly

Username Check

- Check User Names
- Knowem - Search for a username on over 500 popular social networks.
- Linkedin2Username - Web scraper that uses valid LinkedIn credentials to put together a list of employees for a specified company.
- Name Checkr
- Name Checkup
- Name Chk
- User Search

Personal Investigations

- 192 (UK)
- 411 (US)
- Alumni.net
- Ancestry
- Been Verified - Good accuracy, paid person search.
- CVGadget
- Canada411
- Cedar
- Charlie App
- Classmates
- CrunchBase
- Data 24-7
- Family Search
- Family Tree Now
- Federal Bureau of Prisons Inmate Locator (US) - Find an inmate that is in the Federal Bureau of Prisons system.
- Fold3 (US Military Records) - Browse records of US Military members.
- Genealogy Bank
- Genealogy Links
- Go Find Who - Multiple handy search tools.
- Homemetry
- Infobel
- Infospace White Pages
- Interment
- International White and Yellow Pages
- Itools
- Kompass
- Locate Family - Basicly a worldwide phonebook that can be manually searched. This site shows up as results on google.com so searches based on name, address, or phone number.
- LookUpUK
- Lullar
- MelissaDATA
- My Life People Search
- My Life - Paid people search with lots of results.
- PeekYou
- People Search (Australia)
- PeopleSearch.net
- Pipl
- Rapportive
- RecordsPedia
- Recruitem
- Reunion
- Rootsweb
- SearchBug
- Skip Ease
- SnoopStation
- Sowdust Facebook Search - Facebook search tool.
- Spokeo
- That's Them - Good accuracy, paid person search.
- The National Archives (UK)
- USSearch

- WebMiii
- White Pages (US)
- Wink
- Yasni
- Zabasearch
- Zoominfo
- facesearch - Search for images of a person by name.
- snitch.name

E-mail Search / E-mail Check

- BriteVerify Email Verification
- Email Address Validator
- Email Format
- Email Permutator+
- EmailHippo
- EmailSearch.net
- Have I Been Pwned - Search across multiple data breaches to see if your email address has been compromised.
- Hunter - Hunter lets you find email addresses in seconds and connect with the people that matter for your business.
- MailTester
- MyCleanList
- Peepmail
- Pipl
- ReversePhoneCheck
- ThatsThem
- FindEmails.com
- Verify Email
- VoilaNorbert - Find anyone's contact information for lead research or talent acquisition.
- h8mail - Password Breach Hunting and Email OSINT, locally or using premium services. Supports chasing down related email

Phone Number Research

- National Cellular Directory - was created to help people research and reconnect with one another by performing cell phone lookups. The lookup products includes have billions of records that can be accessed at any time, as well as free searches one hour a day, every day.
- Reverse Phone Lookup - Detailed information about phone carrier, region, service provider, and switch information.
- Spy Dialer - Get the voicemail of a cell phone & owner name lookup.
- Twilio - Look up a phone numbers carrier type, location, etc.
- Phone Validator - Pretty accurate phone lookup service, particularly good against Google Voice numbers.

Company Research

- AllStocksLinks
- Battle of the Internet Giants
- Better Business Bureau
- Bizeurope

- Bloomberg
- Business Source
- Bureau Van Dijk
- Canadian Business Research
- Canadian Business Resource
- Central and Eastern European Business Directory
- Company Registration Round the World
- Company Research Resources by Country Comparably
- CompeteShark
- Corporate Information
- CrunchBase
- EDGAR Online
- Europages
- European Business Register
- Ezilon
- Factiva
- Glassdoor
- globalEdge
- GuideStar
- Hoovers
- Inc. 5000
- InstantLogoSearch
- iSpionage
- Knowledge guide to international company registration
- Linkedin
- National Company Registers
- Mergent Intellect
- Mergent Online
- Morningstar Research
- Notablist
- Orbis directory
- opencorporates
- Owler
- Overseas Company Registers
- Plunkett Research
- Scoot
- SEMrush
- Serpstat
- SpyFu
- Forbes Global 2000
- Vault
- Xing

Domain and IP Research

- Accuranker
- ahrefs - A tool for backlink research, organic traffic research, keyword research, content marketing & more.
- Alexa
- Bing Webmaster Tools
- BuiltWith
- Central Ops
- Dedicated or Not

- DNSDumpster
- DNS History
- DNSStuff
- DNSViz
- Domain Big Data
- Domain Crawler
- Domain Dossier
- Domain Tools - Whois lookup and domain/ip historical data.
- Easy whois
- Exonera Tor - A database of IP addresses that have been part of the Tor network. It answers the question whether there was a Tor relay running on a given IP address on a given date.
- Follow.net
- GraphyStories
- HypeStat
- Infosniper
- intoDNS
- IP Checking
- IP Location
- IP 2 Geolocation
- IP 2 Location
- IPFingerprints
- IPVoid - IP address toolset.
- IntelliTamper
- Kloth
- NetworkTools
- Majestic
- MaxMind
- MXToolbox - MX record lookup tool.
- Netcraft Site Report
- OpenLinkProfiler
- Link Explorer
- PageGlimpse
- Pentest-Tools.com
- PhishStats
- Pulsedive
- Quantcast
- Quick Sprout
- RedirectDetective
- Remote DNS Lookup
- Robtex
- SecurityTrails - API to search current and historical DNS records, current and historical WHOIS, technologies used by sites and whois search for phone, email, address, IPs etc.
- SEMrush
- SEOTools for Excel
- Similar Web - Compare any website traffic statistics & analytics.
- SmallSEOTools
- StatsCrop
- Squatm3gator - Enumerate available domains generated modifying the original domain name through different cybersquatting techniques

- URLVoid - Analyzes a website through multiple blacklist engines and online reputation tools to facilitate the detection of fraudulent and malicious websites.
- Wappalyzer
- WebMeUp
- Website Informer
- WhatIsMyIPAddress
- Who.is - Domain whois information.
- Whois Arin Online
- WhoIsHostingThis
- Whoisology
- WhoIsRequest
- w3snoop
- Verisign
- ViewDNS.info
- You Get Signal

Keywords Discovery and Research

- Google Adwords - Get monthly keyword volume data and stats.
- Google Trends - See how many users are searching for specific keywords.
- Keyword Discovery
- Keyword Spy
- KeywordTool
- One Look Reverse Dictionary
- Soovle
- Ubersuggest
- Word Tracker

Web History and Website Capture

- Archive.is
- BlackWidow
- CashedPages
- CachedView
- DomainTools
- Wayback Machine - Explore the history of a website.
- Wayback Machine Archiver

Image Search

- Baidu Images
- Bing Images
- Flickr
- Google Image
- Gramfeed
- Image Identification Project
- Image Raider
- KarmaDecay
- Lycos Image Search
- PhotoBucket
- Picsearch
- PicTriev
- TinEye - Reverse image search engine.

- Websta
- Strokess
- Worldcam
- Yahoo Image Search
- Yandex Images

Image Analysis

- ExifTool
- Ghiro
- ImpulseAdventure
- Jeffreys Image Metadata Viewer
- JPEGsnoop
- Metapicz

Web Monitoring

- Alltop
- Awasu
- Bridge.Leslibres
- Bridge.Suumitsu
- ChangeDetect
- Deltafeed
- Feed43
- FeedBooster
- Feed Exileed
- Feed Filter Maker
- Feedly
- FeedReader
- FetchRSS
- Flipboard
- FollowThatPage
- Google Alerts - A content change detection and notification service.
- InfoMinder
- Mention
- Netvibes
- Newsblur
- OmeaReader
- OnWebChange
- Reeder
- RSS Bridge
- RSS Feed Reader
- RSS Micro
- RSS Search Engine
- RSS Search Hub
- RSSOwl
- Selfoss
- Silobreaker
- Talkwalker
- The Old Reader
- versionista
- visualping
- WebSite Watcher

- Winds

Social Network Analysis

- Gephi
- ORA
- Sentinel Visualizer
- Visual Investigative Scenarios
- Wynyard Group

DNS Search And Enumeration

- Amass - The amass tool searches Internet data sources, performs brute force subdomain enumeration, searches web archives, and uses machine learning to generate additional subdomain name guesses. DNS name resolution is performed across many public servers so the authoritative server will see the traffic coming from different locations. Written in Go.

Network Reconnaissance Tools

- ACLight - Script for advanced discovery of sensitive Privileged Accounts - includes Shadow Admins.
- BuiltWith - Technology lookup tool for websites.
- CloudFail - Unmask server IP addresses hidden behind Cloudflare by searching old database records and detecting misconfigured DNS.
- LdapMiner - Multiplatform LDAP enumeration utility.
- Mass Scan - TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.
- Netdiscover - Simple and quick network scanning tool.
- Pentest-Tools - Online suite of various different pentest related tools.
- Ruler - Tool for remotely interacting with Exchange servers.
- Shodan - Database containing information on all accessible domains on the internet obtained from passive scanning.
- Spyse - Web research services that scan the entire internet using OSINT, to simplify the investigation of infrastructure and attack surfaces.
- Spyse.py - Python API wrapper and command-line client for the tools hosted on spyse.com.
- Sublist3r - Subdomain enumeration tool for penetration testers.
- ldapsearch - Linux command line utility for querying LDAP servers.
- nmap - Free security scanner for network exploration & security audits.
- pyShodan - Python 3 script for interacting with Shodan API (requires valid API key).
- smbmap - Handy SMB enumeration tool.
- xprobe2 - Open source operating system fingerprinting tool.
- zmap - Open source network scanner that enables researchers to easily perform Internet-wide network studies.

Exploitation Enumeration And Data Recovery Tools

Penetration Testing OS Distributions

- ArchStrike - Arch GNU/Linux repository for security professionals and enthusiasts.

- AttifyOS - GNU/Linux distribution focused on tools useful during Internet of Things (IoT) security assessments.
- BackBox - Ubuntu-based distribution for penetration tests and security assessments.
- BlackArch - Arch GNU/Linux-based distribution for penetration testers and security researchers.
- Buscador - GNU/Linux virtual machine that is pre-configured for online investigators.
- Fedora Security Lab - Provides a safe test environment to work on security auditing, forensics, system rescue and teaching security testing methodologies.
- Kali - GNU/Linux distribution designed for digital forensics and penetration testing.
- Network Security Toolkit (NST) - Fedora-based bootable live operating system designed to provide easy access to best-of-breed open source network security applications.
- Parrot Security OS - Distribution similar to Kali using the same repositories, but with additional features such as Tor and I2P integration.
- The Pentesters Framework - Distro organized around the Penetration Testing Execution Standard (PTES), providing a curated collection of utilities that eliminates often unused toolchains.

Multi-paradigm Frameworks

- Armitage - Java-based GUI front-end for the Metasploit Framework.
- AutoSploit - Automated mass exploiter, which collects target by employing the Shodan.io API and programmatically chooses Metasploit exploit modules based on the Shodan query.
- Faraday - Multiuser integrated pentesting environment for red teams performing cooperative penetration tests, security audits, and risk assessments.
- Habu Hacking Toolkit - Unified set of tools spanning passive reconnaissance, network attacks, social media monitoring, and website fingerprinting.
- Mad-Metasploit - Additional scripts for Metasploit.
- Metasploit - Software for offensive security teams to help verify vulnerabilities and manage security assessments.
- Mobile Security Framework (MobSF) - Automated mobile application pentesting framework capable of static analysis, dynamic analysis, malware analysis, and web API testing.
- Pupy - Cross-platform (Windows, Linux, macOS, Android) remote administration and post-exploitation tool.
- Rupture - Multipurpose tool capable of man-in-the-middle attacks, BREACH attacks and other compression-based crypto attacks.

Network Vulnerability Scanners

- Nessus - Commercial network vulnerability scanner.
- Nexpose - Commercial vulnerability and risk management assessment engine that integrates with Metasploit, sold by Rapid7.
- OpenVAS - Open source implementation of the popular Nessus vulnerability assessment system.
- Vuls - Agentless Linux/FreeBSD vulnerability scanner written in Go.

Web Vulnerability Scanners

- ACSTIS - Automated client-side template injection (sandbox escape/bypass) detection for AngularJS.
- Burp Suite - Commercial web vulnerability scanner, with limited community edition.
- cms-explorer - Reveal the specific modules, plugins, components and themes that various websites powered by content management systems are running.
- Netsparker Web Application Security Scanner - Commercial web application security scanner to automatically find many different types of security flaws.
- Nikto - Noisy but fast black box web server and web application vulnerability scanner.
- Observatory - Free online web scanning utility.
- OWASP Zed Attack Proxy (ZAP) - Feature-rich, scriptable HTTP intercepting proxy and fuzzer for penetration testing web applications.
- Security Headers - Free online utility for checking a website's HTTP headers for security vulnerabilities.
- SQLmate - A friend of sqlmap that identifies sqli vulnerabilities based on a given dork and website (optional).
- WPScan - Black box WordPress vulnerability scanner.

Web Exploitation

- Browser Exploitation Framework (BeEF) - Command and control server for delivering exploits to commandeered Web browsers.
- Commix - Automated all-in-one operating system command injection and exploitation tool.
- Drupwn - Drupal web application exploitation tool.
- EyeWitness - Tool to take screenshots of websites, provide some server header info, and identify default credentials if possible.
- fimap - Find, prepare, audit, exploit and even Google automatically for LFI/RFI bugs.
- FuzzDB - Dictionary of attack patterns and primitives for black-box application fault injection and resource discovery.
- IIS-Shortname-Scanner - Command line tool to exploit the Windows IIS tilde information disclosure vulnerability.
- Kadabra - Automatic LFI exploiter and scanner.
- Kadimus - LFI scan and exploit tool.
- LFISuite - A tool designed to exploit Local File Include vulnerabilities.
- libformatstr - Python script designed to simplify format string exploits.
- liffy - LFI exploitation tool.
- lyncsmash - A collection of tools to enumerate and attack self-hosted Skype for Business and Microsoft Lync installations
- NoSQLmap - Automatic NoSQL injection and database takeover tool.
- SQLmap - Automated SQL injection and database takeover tool.
- sqlninja - Automated SQL injection and database takeover tool.
- sslstrip2 - SSLStrip version to defeat HSTS.
- sslstrip - Demonstration of the HTTPS stripping attacks.
- tplmap - Automatic server-side template injection and Web server takeover tool.
- VHostScan - A virtual host scanner that performs reverse lookups, can be used with pivot tools, detect catch-all scenarios, aliases and dynamic default pages.
- wafw00f - Identifies and fingerprints Web Application Firewall (WAF) products.
- webscreenshot - A simple script to take screenshots from a list of websites.
- weevely3 - Weaponized web shell.

- Wordpress Exploit Framework - Ruby framework for developing and using modules which aid in the penetration testing of WordPress powered websites and systems.
- WPSploit - Exploit WordPress-powered websites with Metasploit.

Network Tools

- dnstwist - Domain name permutation engine for detecting typo squatting, phishing and corporate espionage.
- dsniff - Collection of tools for network auditing and pentesting.
- enumdb - MySQL and MSSQL bruteforce utility
- FireAway - Firewall audit and security bypass tool.
- impacket - Collection of Python classes for working with network protocols.
- Intercepter-NG - Multifunctional network toolkit.
- kerbrute - A tool to perform Kerberos pre-auth bruteforcing.
- Low Orbit Ion Cannon (LOIC) - Open source network stress testing tool.
- Ncat - TCP/IP command line utility supporting multiple protocols.
- netcut - ARP based utility for discovering and spoofing MAC addresses and enabling/disabling network connectivity on network devices.
- Network-Tools.com - Website offering an interface to numerous basic network utilities like `ping`, `traceroute`, `whois`, and more.
- patator - Patator is a multi-purpose brute-forcer, with a modular design and a flexible usage.
- pig - GNU/Linux packet crafting tool.
- Praeda - Automated multi-function printer data harvester for gathering usable data during security assessments.
- Printer Exploitation Toolkit (PRET) - Tool for printer security testing capable of IP and USB connectivity, fuzzing, and exploitation of PostScript, PJL, and PCL printer language features.
- routersploit - Open source exploitation framework similar to Metasploit but dedicated to embedded devices.
- scapy - Python-based interactive packet manipulation program & library.
- Sockstress - TCP based DoS utility.
- SPARTA - Graphical interface offering scriptable, configurable access to existing network infrastructure scanning and enumeration tools.
- Spyse - Web research services that scan the entire internet using OSINT, to simplify the investigation of infrastructure and attack surfaces.
- Spyse.py - Python API wrapper and command-line client for the tools hosted on spyse.com.
- THC Hydra - Online password cracking tool with built-in support for many network protocols, including HTTP, SMB, FTP, telnet, ICQ, MySQL, LDAP, IMAP, VNC, and more.
- UFONet - Layer 7 DDoS/DoS tool.
- Zarp - Multipurpose network attack tool, both wired and wireless.

Protocol Analyzers and Sniffers

- tcpdump/libpcap - Common packet analyzer that runs under the command line.
- Wireshark - Widely-used graphical, cross-platform network protocol analyzer.
- Yersinia - Packet and protocol analyzer with MITM capability.
- Fiddler - Cross platform packet capturing tool for capturing HTTP/HTTPS traffic.
- netsniff-ng - Swiss army knife for Linux network sniffing.
- Dshell - Network forensic analysis framework.

- Chaosreader - Universal TCP/UDP snarfing tool that dumps session data from various protocols.

Proxies and MITM Tools

- BetterCAP - Modular, portable and easily extensible MITM framework.
- dnschef - Highly configurable DNS proxy for pentesters.
- Ettercap - Comprehensive, mature suite for machine-in-the-middle attacks.
- evilgrade - Modular framework to take advantage of poor upgrade implementations by injecting fake updates.
- mallory - HTTP/HTTPS proxy over SSH
- MITMf - Multipurpose man-in-the-middle framework.
  - e.g. `mitmf --arp --spoof -i eth0 --gateway 192.168.1.1 --targets 192.168.1.20 --inject --js-url http://192.168.1.137:3000/hook.js`
- mitmproxy - Interactive TLS-capable intercepting HTTP proxy for penetration testers and software developers.
- Morpheus - Automated ettercap TCP/IP Hijacking tool.
- Responder-Windows - Windows version of the above NBT-NS/LLMNR/MDNS poisoner.
- Responder - Open source NBT-NS, LLMNR, and MDNS poisoner.
- SSH MITM - Intercept SSH connections with a proxy; all plaintext passwords and sessions are logged to disk.

Wireless Network Tools

- Aircrack-ng - Set of tools for auditing wireless networks.
- BetterCAP - Wifi, Bluetooth LE, and HID reconnaissance and MITM attack framework, written in Go.
- Fluxion - Suite of automated social engineering based WPA attacks.
- Kismet - Wireless network discovery tool.
- MANA Toolkit - Rogue AP and man-in-the-middle utility.
- NetStumbler - WLAN scanning tool.
- WiFi Pumpkin - All in one Wi-Fi exploitation and spoofing utility.
- wifi-pickle - Fake access point attacks.
- Wifite - Automated wireless attack tool.

Transport Layer Security Tools

- tlssled - Comprehensive TLS/SSL testing suite.
- SSLscan - Quick command line SSL/TLS analyzer.
- SSLyze - Fast and comprehensive TLS/SSL configuration analyzer to help identify security mis-configurations.
- SSL Labs - Online TLS/SSL testing suite for revealing supported TLS/SSL versions and ciphers.
- crackpkcs12 - Multithreaded program to crack PKCS#12 files (`.p12` and `.pfx` extensions), such as TLS/SSL certificates.
- spoodle - Mass subdomain + POODLE vulnerability scanner.
- SMTP TLS Checker - Online TLS/SSL testing suite for SMTP servers.

Cryptography

- FeatherDuster - Analysis tool for discovering flaws in cryptography.
- rsatool - Tool for calculating RSA and RSA-CRT parameters.
- xortool - XOR cipher analysis tool.

Post-Exploitation

- CrackMapExec - Multipurpose post-exploitation suite containing many plugins.
- DBC2 - Multipurpose post-exploitation tool.
- Empire - PowerShell based (Windows) and Python based (Linux/OS X) post-exploitation framework.
- EvilOSX - macOS backdoor with docker support.
- Fathomless - A collection of post-exploitation tools for both Linux and Windows systems.
- FruityC2 - Open source, agent-based post-exploitation framework with a web UI for management.
- Koadic - Windows post-exploitation rootkit, primarily utilizing Windows Script Host.
- PlugBot - Can be installed onto an ARM device for Command & Control use and more.
- Portia - Automated post-exploitation tool for lateral movement and privilege escalation.
- ProcessHider - Post-exploitation tool for hiding processes.
- Pupy - Open source cross-platform post-exploitation tool, mostly written in Python.
- RemoteRecon - Post-exploitation utility making use of multiple agents to perform different tasks.
- TheFatRat - Tool designed to generate remote access trojans (backdoors) with msfvenom.arch-project/) - Can be installed onto an ARM device for Command & Control use and more.
- p0wnedShell - PowerShell based post-exploitation utility utilizing .NET.
- poet - Simple but multipurpose post-exploitation tool.

Exfiltration Tools

- Data Exfiltration Toolkit (DET) - Proof of concept to perform data exfiltration using either single or multiple channel(s) at the same time.
- dnsteal - Fake DNS server for stealthily extracting files.
- HTTPTunnel - Tunnel data over pure HTTP GET/POST requests.
- Iodine - Tunnel IPv4 data through a DNS server; useful for exfiltration from networks where Internet access is firewalled, but DNS queries are allowed.
- MailSniper - Search through email in a Microsoft Exchange environment for specific terms (passwords, insider intel, network architecture information, etc.).
- mallory - HTTP/HTTPS proxy over SSH.
- mimikatz - Credentials extraction tool for Windows operating system.
- mimikittenz - Post-exploitation PowerShell tool for extracting data from process memory.
- PANHunt - Search file systems for credit cards.
- PassHunt - Search file systems for passwords.
- ptunnel-ng - Tunnel IPv4 traffic through ICMP pings; slow but stealthy when normal IP exfiltration traffic is blocked.
- pwnat - Punches holes in firewalls and NATs.
- spYDyishai - Local Google credentials exfiltration tool, written in Python.
- tgcd - Simple Unix network utility to extend the accessibility of TCP/IP based network services beyond firewalls.

Static Analyzers

- Androbugs-Framework - Android program vulnerability analysis tool.
- Androwarn - Android static code analysis tool.
- APKinspector - Android APK analysis tool with GUI.
- bandit - Security oriented static analyser for python code.
- Brakeman - Static analysis security vulnerability scanner for Ruby on Rails applications.
- Codebeat (open source) - Open source implementation of commercial static code analysis tool with GitHub integration.
- Codelyzer - A set of tslint rules for static code analysis of Angular TypeScript projects. You can run the static code analyzer over web apps, NativeScript, Ionic, etc.
- cppcheck - Extensible C/C++ static analyzer focused on finding bugs.
- FindBugs - Free software static analyzer to look for bugs in Java code.
- Icewater - 16,432 free Yara rules.
- Joint Advanced Defense Assessment for Android Applications (JAADAS) - Multipurpose Android static analysis tool.
- OWASP Dependency Check - Open source static analysis tool that enumerates dependencies used by Java and .NET software code (with experimental support for Python, Ruby, Node.js, C, and C++) and lists security vulnerabilities associated with the depedencies.
- pefile - Static portable executable file inspector.
- Progpilot - Static security analysis tool for PHP code.
- Quick Android Review Kit (Qark) - Tool for finding security related Android application vulnerabilities.
- ShellCheck - Static code analysis tool for shell script.
- smalisca - Android static code analysis tool.
- sobelow - Security-focused static analysis for the Phoenix Framework.
- truffleHog - Git repo scanner.
- Veracode - Commercial cloud platform for static code analysis, dynamic code analysis, dependency/plugin analysis, and more.
- VisualCodeGrepper - Open source static code analysis tool with support for Java, C, C++, C#, PL/SQL, VB, and PHP. VisualCodeGrepper also conforms to OWASP best practices.
- Yara - Static pattern analysis tool for malware researchers.

Dynamic Analyzers

- AndroidHooker - Dynamic Android application analysis tool.
- Androl4b - Android security virtual machine based on Ubuntu-MATE for reverse engineering and malware analysis.
- Cheat Engine - Memory debugger and hex editor for running applications.
- ConDroid - Android dynamic application analysis tool.
- Cuckoo - Automated dynamic malware analysis tool.
- DECAF - Dynamic code analysis tool.
- droidbox - Dynamic malware analysis tool for Android, extension to DECAF.
- drozer - Android platform dynamic vulnerability assessment tool.
- idb - iOS app security analyzer.
- Inspeckage - Dynamic Android package analysis tool.

Hex Editors

- Cheat Engine - Memory debugger and hex editor for running applications.
- Frhed - Binary file editor for Windows.

- HexEdit.js - Browser-based hex editing.
- Hexinator - World's finest (proprietary, commercial) Hex Editor.

File Format Analysis Tools

- Hachoir - Python library to view and edit a binary stream as tree of fields and tools for metadata extraction.
- Kaitai Struct - File formats and network protocols dissection language and web IDE, generating parsers in C++, C#, Java, JavaScript, Perl, PHP, Python, Ruby.
- Veles - Binary data visualization and analysis tool.

Anti-Virus Evasion Tools

- AntiVirus Evasion Tool (AVET) - Post-process exploits containing executable files targeted for Windows machines to avoid being recognized by antivirus software.
- Hyperion - Runtime encryptor for 32-bit portable executables ("PE `.exe`s").
- peCloak.py - Automates the process of hiding a malicious Windows executable from antivirus (AV) detection.
- peCloakCapstone - Multi-platform fork of the peCloak.py automated malware antivirus evasion tool.
- Shellter - Dynamic shellcode injection tool, and the first truly dynamic PE infector ever created.
- SigThief - Stealing signatures to evade AV.
- UniByAv - Simple obfuscator that takes raw shellcode and generates Anti-Virus friendly executables by using a brute-forcable, 32-bit XOR key.
- Windows-SignedBinary - AV evasion tool for binary files.

Hash Cracking Tools

- CeWL - Generates custom wordlists by spidering a target's website and collecting unique words.
- CrackStation - Online password cracker.
- Hashcat - Fast hash cracking utility with support for most known hashes as well as OpenCL and CUDA acceleration.
- John the Ripper Jumbo edition - Community enhanced version of John the Ripper.
- John the Ripper - Fast password cracker.
- JWT Cracker - Simple HS256 JWT token brute force cracker.
- Mentalist - Unique GUI based password wordlist generator compatible with CeWL and John the Ripper.
- JPassword Recovery Tool - RAR bruteforce cracker. Formery named RAR Crack.

Windows Utilities

- Bloodhound - Graphical Active Directory trust relationship explorer.
- Commentator - PowerShell script for adding comments to MS Office documents, and these comments can contain code to be executed.
- DeathStar - Python script that uses Empire's RESTful API to automate gaining Domain Admin rights in Active Directory environments.
- Empire - Pure PowerShell post-exploitation agent.
- Fibratus - Tool for exploration and tracing of the Windows kernel.
- GetVulnerableGPO - PowerShell based utility for finding vulnerable GPOs.
- Headstart - Lazy man's Windows privilege escalation tool utilizing PowerSploit.
- Hyena - NetBIOS exploitation.

- Luckystrike - PowerShell based utility for the creation of malicious Office macro documents.
- Magic Unicorn - Shellcode generator for numerous attack vectors, including Microsoft Office macros, PowerShell, HTML applications (HTA), or `certutil` (using fake certificates).
- Mimikatz - Credentials extraction tool for Windows operating system.
- PowerSploit - PowerShell Post-Exploitation Framework.
- PSKernel-Primitives - Exploiting primitives for PowerShell.
- Redsnarf - Post-exploitation tool for retrieving password hashes and credentials from Windows workstations, servers, and domain controllers.
- Rubeus - Rubeus is a C# toolset for raw Kerberos interaction and abuses.
- Sysinternals Suite - The Sysinternals Troubleshooting Utilities.
- Windows Credentials Editor - Inspect logon sessions and add, change, list, and delete associated credentials, including Kerberos tickets.
- Windows Exploit Suggester - Suggests Windows exploits based on patch levels.

GNU Linux Utilities

- Linus - Security auditing tool for Linux and macOS.
- Linux Exploit Suggester - Heuristic reporting on potentially viable exploits for a given GNU/Linux system.
- Mempodipper - Linux Kernel 2.6.39 < 3.2.2 local privilege escalation script.
- vuls - Linux/FreeBSD agentless vulnerability scanner.

macOS Utilities

- Bella - Bella is a pure python post-exploitation data mining tool & remote administration tool for macOS.
- Linus - Security auditing tool for Linux and macOS.

Social Engineering Tools

- Beelogger - Tool for generating keylooger.
- Catphish - Tool for phishing and corporate espionage written in Ruby.
- Evilginx - MITM attack framework used for phishing credentials and session cookies from any Web service
- Gophish - Open-Source Phishing Framework
- King Phisher - Phishing campaign toolkit used for creating and managing multiple simultaneous phishing attacks with custom email and server content.
- Lucy Phishing Server - (commercial) tool to perform security awareness trainings for employees including custom phishing campaigns, malware attacks etc. Includes many useful attack templates as well as training materials to raise security awareness.
- PhishingFrenzy - Phishing Frenzy is an Open Source Ruby on Rails application that is leveraged by penetration testers to manage email phishing campaigns.
- SET - The Social-Engineer Toolkit from TrustedSec
- wifiphisher - Automated phishing attacks against Wi-Fi networks
- Canary Tokens - Generate tokens to automatically alert users when triggered.

Anonymity Tools

- Freenet - Freenet is a peer-to-peer platform for censorship-resistant communication and publishing.
- I2P - The Invisible Internet Project.

- OnionScan - Tool for investigating the Dark Web by finding operational security issues introduced by Tor hidden service operators.
- Tor - Free software and onion routed overlay network that helps you defend against traffic analysis.
- What Every Browser Knows About You - Comprehensive detection page to test your own Web browser's configuration for privacy and identity leaks.

Reverse Engineering Tools

- Balbuzard - Malware analysis tool with reverse obfuscation.
- binwalk - Fast, easy to use tool for analyzing, reverse engineering, and extracting firmware images.
- Capstone - Lightweight multi-platform, multi-architecture disassembly framework.
- Cuckoo Modified API - Python API for Cuckoo Modified.
- Cuckoo Modified - Fork of Cuckoo Sandbox with multiple improvements.
- Cuckoo Sandbox - Online malware scanner.
- de4dot - .NET deobfuscator and unpacker.
- dnSpy - Tool to reverse engineer .NET assemblies.
- [Dovehawk] (https://github.com/tylabs/dovehawk) - Dovehawk is a Zeek module that automatically imports MISP indicators and reports Sightings
- DRAKVUF - Virtualization based agentless black-box binary analysis system.
- Evan's Debugger - OllyDbg-like debugger for GNU/Linux.
- FireEye Labs Obfuscated String Solver (FLOSS) - Malware deobfuscator.
- firmware.re - Firmware analyzier.
- HaboMalHunter - Automated malware analysis tool for Linux ELF files.
- Hybrid Analysis - Online malware scanner.
- Immunity Debugger - Powerful way to write exploits and analyze malware.
- Interactive Disassembler (IDA Pro) - Proprietary multi-processor disassembler and debugger for Windows, GNU/Linux, or macOS; also has a free version, IDA Free.
- Malaice.io - Open source malware analyzer.
- Malheur - Automated sandbox analysis of malware behavior.
- Medusa - Open source, cross-platform interactive disassembler.
- Metadefender - Online file and hash analyzer.
- NoMoreXOR - Frequency analysis tool for trying to crack 256-bit XOR keys.
- OllyDbg - x86 debugger for Windows binaries that emphasizes binary code analysis.
- PackerAttacker - Generic hidden code extractor for Windows malware.
- PacketTotal - Online pcap file analyzer.
- peda - Python Exploit Development Assistance for GDB.
- plasma - Interactive disassembler for x86/ARM/MIPS. Generates indented pseudo-code with colored syntax code.
- PyREBox - Python scriptable Reverse Engineering sandbox by Cisco-Talos.
- Radare2 - Open source, crossplatform reverse engineering framework.
- Ragpicker - Malware analysis tool.
- rVMI - Debugger on steroids; inspect userspace processes, kernel drivers, and preboot environments in a single tool.
- Sandboxed Execution Environment - Framework for building sandboxed malware execution environments.
- unXOR - Tool that guesses XOR keys using known plaintext attacks.
- VirtualDeobfuscator - Reverse engineering tool for virtualization wrappers.
- VirusTotal - Online malware scanner.
- Voltron - Extensible debugger UI toolkit written in Python.

- WDK/WinDbg - Windows Driver Kit and WinDbg.
- x64dbg - Open source x64/x32 debugger for windows.
- xortool - Tool for guessing XOR keys.

Side-channel Tools

- ChipWhisperer - Complete open-source toolchain for side-channel power analysis and glitching attacks.

Forensic Tools

- Appliance for Digital Investigation and Analysis (ADIA) - VMware virtual appliance for digital forensics.
- Autopsy - Graphical interface to The Sleuth Kit.
- binwalk - Firmware analysis tool.
- bulk_extractor - Command line tool for extracting email addresses, credit card numbers, URLs, and other types of information from many types of files, including compressed files and images.
- CAINE - Italian live Linux distro for digital forensics.
- chkrootkit - Checks local Linux systems for rootkits.
- Chrome URL Dumper - Python based agent that gathers and dumps Chrome history (URLs).
- DEFT Linux - Linux distro for digital forensics analysis.
- Digital Forensics Framework (DFF) - Open source digital forensics framework with GUI.
- docker-explorer - Docker file system forensic tool.
- Dumpzilla - Python based application for dumping information from Firefox, Iceweasel, and Seamonkey browsers.
- extundelete - ext3 and ext4 file recovery tool.
- Fast Evidence Collector Toolkit (FECT) - Lightweight digital forensics tool.
- FireEye Labs Obfuscated String Solver (FLOSS) - Extract obfuscated strings from malware.
- Foremost - File recovery tool.
- GRR Rapid Response - Incident response framework focused on remote live forensics.
- Hindsight - Chrome/Chromium browser forensics tool.
- IREC - All in one evidence collector.
- Linux Expl0rer - Easy-to-use live forensics toolbox for Linux endpoints written in Python & Flask.
- magneto-malware-scanner - Malware scanning platform.
- nightHawk - Platform for digital forensics presentation, using Elasticsearch.
- PALADIN - Linux distro for digital forensics.
- pdf-parser - PDF digital forensics software.
- pdfid - PDF digital forensics software.
- pdfminer - Tool for extracting information from the text of PDF documents.
- peepdf - Python PDF analysis tool.
- PowerForensics - PowerShell based digital forensics suite.
- PSRecon - Windows based data gathering tool using PowerShell.
- Regripper - Windows Registry data extraction tool.
- Rekall - Incident response and forensics tool.
- SANS Investigative Forensics Toolkit (SIFT) - Linux VM for digital forensics.
- SIFT Workstation - Linux distro (with optional VM) for digital forensics.

- The Sleuth Kit - Collection of command line digital forensic utilities for investigating disk images, volume and file system data, and more.

Memory Analysis

- Evolve - Web interface for Volatility advanced memory forensics framework.
- inVtero.net - Windows x64 memory analysis tool.
- Linux Memory Extractor (LiME) - A Loadable Kernel Module (LKM) allowing for volatile memory extraction of Linux-based systems.
- Memoryze - Memory forensics software.
- Microsoft User Mode Process Dumping - Dumps any running Win32 processes memory image on the fly.
- PMDump - Tool for dumping memory contents of a process without stopping the process.
- Rekall - Open source tool and library for the extraction of digital artifacts from volatile memory, RAM, samples.
- Responder PRO - Commercial memory analysis software.
- Volatility - Advanced memory forensics framework.
- VolatilityBot - Automation tool utilizing Volatility.
- VolDiff - Malware Memory Footprint Analysis based on Volatility.
- WindowsSCOPE - Commercial memory forensics software for Windows systems.

Memory Imaging Tools

- Belkasoft Live RAM Capturer - A tiny free forensic tool to reliably extract the entire content of the computer's volatile memory – even if protected by an active anti-debugging or anti-dumping system.
- Linux Memory Grabber - A script for dumping Linux memory and creating Volatility profiles.
- Magnet RAM Capture - Magnet RAM Capture is a free imaging tool designed to capture the physical memory of a suspect's computer. Supports recent versions of Windows.
- OSForensics - OSForensics can acquire live memory on 32bit and 64bit systems. A dump of an individual process's memory space or physical memory dump can be done.

Incident Response

- APT Simulator - Windows Batch Script that makes a system appear compromised.
- Atomic Red Team - Set of premade tests to evaluate security posture.
- AutoTTP - Automated Tactics Techniques & Procedures, for re-issuing complex tasks.
- Belkasoft Evidence Center - Commercial incident response suite.
- Blue Team Training Toolkit - Toolkit for preparing blue teams for defensive security.
- Caldera - Automated adversary emulation system.
- CIRTKit - Open source incident response framework.
- Cyber Triage - Commercial incident response suite.
- Doorman - Osquery fleet manager.
- DumpsterFire Toolset - Security event simulator.
- Falcon Orchestrator - Windows based incident management framework.
- GRR Rapid Response - Python based incident mangement framework.
- Kolide Fleet - Open source osquery manager.

- LimaCharlie - Cross-platform open source endpoint detection and response solution.
- Metta - Open source adversary simulation.
- MIG - Mozilla InvestiGator - Endpoint inspection.
- MozDef - Mozilla defense platform.
- Network Flight Simulator - Utility for generating malicious network traffic.
- Osquery - Multiplatform framework for querying operating systems similar to SQL queries.
- Red Team Automation (RTA) - Adversary simulation framework.
- RedHunt OS - Purposely vulnerable Linux VM.
- Redline - Investigative tool able to scan processes, memory, file system metadata, and more.
- Zentral - Monitors system events using osquery.

Honeypot Tools

- bap - Basic Authentication honeyPot - HTTP basic authentication web service honeypot.
- conpot - ICS/SCADA honeypot.
- Cowrie Docker - Docker version of Cowrie, SSH/Telnet honeypot.
- Cowrie - SSH/Telnet honeypot.
- dionaea - Multipurpose honeypot.
- elastichoney - Elasticsearch honeypot.
- glastopf - Python based web application honeypot.
- glutton - Multipurpose honeypot.
- Modern Honey Network (mhn) - Multipurpose honeypot with centralized management and many integrations.
- MongoDB-HoneyProxy - MongoDB honeypot.
- MysqlPot - MySQL honeypot.
- Nodepot - NodeJS web application honeypot.
- Nosqlpot - NoSQL honeypot.
- phpmyadmin_honeypot - PHPMyAdmin honeypot.
- Servletpot - Web application honeypot written in Java, making use of Apache HttpClient libraries, MySQL connector, Cassandra connector.
- Shadow Daemon - Collection of tools to detect, record, and prevent attacks on web applications.
- smart-honeypot - PHP based honeypot.
- SpamScope - Spam analysis tool.
- Thug - Python based honeyclient tool.
- Wordpot - WordPress honeypot.
- wp-smart-honeypot - WordPress plugin and honeypot designed to reduce comment spam.

Monitoring and IDS-IPS

- AIEngine - Very advanced NIDS.
- Elastic Stack - Also known as the ELK stack, the combination of Elasticsearch, Logstash, and Kibana, for monitoring and logging.
- OSSEC - Open source HIDS.
- Security Onion - Linux distro for monitoring.
- Snort - Open source NIPS/NIDS.
- SSHWATCH - SSH IPS.
- Suricata - Open source NIPS/NIDS.

Physical Tools

- LAN Turtle - Covert "USB Ethernet Adapter" that provides remote access, network intelligence gathering, and MITM capabilities when installed in a local network.
- PCILeech - Uses PCIe hardware devices to read and write from the target system memory via Direct Memory Access (DMA) over PCIe.
- Poisontap - Siphons cookies, exposes internal (LAN-side) router and installs web backdoor on locked computers.
- Proxmark3 - RFID/NFC cloning, replay, and spoofing toolkit often used for analyzing and attacking proximity cards/readers, wireless keys/keyfobs, and more.
- USB Rubber Ducky - Customizable keystroke injection attack platform masquerading as a USB thumbdrive.
- WiFi Pineapple - Wireless auditing and penetration testing platform.

Adversary Emulation

- APTSimulator - A Windows Batch script that uses a set of tools and output files to make a system look as if it was compromised.
- Atomic Red Team](https://github.com/redcanaryco/atomic-red-team) - Small and highly portable detection tests mapped to the Mitre ATT&CK Framework.
- AutoTTP - Automated Tactics Techniques & Procedures. Re-running complex sequences manually for regression tests, product evaluations, generate data for researchers.
- Blue Team Training Toolkit](https://www.bt3.no/) - Software for defensive security training, which will bring your network analysis training sessions, incident response drills and red team engagements to a new level.
- Caldera - an automated adversary emulation system that performs post-compromise adversarial behavior within Windows Enterprise networks. It generates plans during operation using a planning system and a pre-configured adversary model based on the Adversarial Tactics, Techniques & Common Knowledge](ATT&CK™) project.
- DumpsterFire - The DumpsterFire Toolset is a modular, menu-driven, cross-platform tool for building repeatable, time-delayed, distributed security events. Easily create custom event chains for Blue Team drills and sensor / alert mapping. Red Teams can create decoy incidents, distractions, and lures to support and scale their operations.
- Metta - An information security preparedness tool to do adversarial simulation.
- Network Flight Simulator - flightsim is a lightweight utility used to generate malicious network traffic and help security teams to evaluate security controls and network visibility.
- Red Team Automation](https://github.com/endgameinc/RTA) - RTA provides a framework of scripts designed to allow blue teams to test their detection capabilities against malicious tradecraft, modeled after MITRE ATT&CK.
- RedHunt-OS - A virtual machine for adversary emulation and threat hunting.

All in one Incident Response Tools

- Belkasoft Evidence Center - The toolkit will quickly extract digital evidence from multiple sources by analyzing hard drives, drive images, memory dumps, iOS, Blackberry and Android backups, UFED, JTAG and chip-off dumps.

- CimSweep - CimSweep is a suite of CIM/WMI-based tools that enable the ability to perform incident response and hunting operations remotely across all versions of Windows.
- CIRTkit - CIRTKit is not just a collection of tools, but also a framework to aid in the ongoing unification of Incident Response and Forensics investigation processes.
- Cyber Triage - Cyber Triage remotely collects and analyzes endpoint data to help determine if it is compromised. It's agentless approach and focus on ease of use and automation allows companies to respond without major infrastructure changes and without a team of forensics experts. Its results are used to decide if the system should be erased or investigated further.
- Digital Forensics Framework - DFF is an Open Source computer forensics platform built on top of a dedicated Application Programming Interface. DFF proposes an alternative to the aging digital forensics solutions used today. Designed for simple use and automation, the DFF interface guides the user through the main steps of a digital investigation so it can be used by both professional and non-expert to quickly and easily conduct a digital investigations and perform incident response.
- Doorman - Doorman is an osquery fleet manager that allows remote management of osquery configurations retrieved by nodes. It takes advantage of osquery's TLS configuration, logger, and distributed read/write endpoints, to give administrators visibility across a fleet of devices with minimal overhead and intrusiveness.
- Envdb - Envdb turns your production, dev, cloud, etc environments into a database cluster you can search using osquery as the foundation. It wraps the osquery process with a cluster node agent that can communicate back to a central location.
- Falcon Orchestrator - Falcon Orchestrator by CrowdStrike is an extendable Windows-based application that provides workflow automation, case management and security response functionality.
- GRR Rapid Response - GRR Rapid Response is an incident response framework focused on remote live forensics. It consists of a python agent client that is installed on target systems, and a python server infrastructure that can manage and talk to the agent.
- Kolide Fleet - Kolide Fleet is a state of the art host monitoring platform tailored for security experts. Leveraging Facebook's battle-tested osquery project, Kolide delivers fast answers to big questions.
- Limacharlie - an endpoint security platform. It is itself a collection of small projects all working together, and gives you a cross-platform, Windows, OSX, Linux, Android and iOS, low-level environment allowing you to manage and push additional modules into memory to extend its functionality.
- MIG - Mozilla Investigator, MIG, is a platform to perform investigative surgery on remote endpoints. It enables investigators to obtain information from large numbers of systems in parallel, thus accelerating investigation of incidents and day-to-day operations security.
- MozDef - The Mozilla Defense Platform, MozDef, seeks to automate the security incident handling process and facilitate the real-time activities of incident handlers.
- nightHawk - the nightHawk Response Platform is an application built for asynchronus forensic data presentation using ElasticSearch as the backend. It's designed to ingest Redline collections.
- Open Computer Forensics Architecture - Open Computer Forensics Architecture, OCFA, is another popular distributed open-source computer forensics framework.

This framework was built on Linux platform and uses postgreSQL database for storing data.

- Osquery - with osquery you can easily ask questions about your Linux and OSX infrastructure. Whether your goal is intrusion detection, infrastructure reliability, or compliance, osquery gives you the ability to empower and inform a broad set of organizations within your company. Queries in the -incident-response pack - help you detect and respond to breaches.
- Redline - provides host investigative capabilities to users to find signs of malicious activity through memory and file analysis, and the development of a threat assessment profile.
- The Sleuth Kit & Autopsy - The Sleuth Kit is a Unix and Windows based tool which helps in forensic analysis of computers. It comes with various tools which helps in digital forensics. These tools help in analyzing disk images, performing in-depth analysis of file systems, and various other things.
- TheHive - TheHive is a scalable 3-in-1 open source and free solution designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.
- X-Ways Forensics - X-Ways is a forensics tool for Disk cloning and imaging. It can be used to find deleted files and disk analysis.
- Zentral - combines osquery's powerful endpoint inventory features with a flexible notification and action framework. This enables one to identify and react to changes on OS X and Linux clients.

Disk Image Creation Tools

- AccessData FTK Imager - AccessData FTK Imager is a forensics tool whose main purpose is to preview recoverable data from a disk of any kind. FTK Imager can also acquire live memory and paging file on 32bit and 64bit systems.
- Bitscout - Bitscout by Vitaly Kamluk helps you build your fully-trusted customizable LiveCD/LiveUSB image to be used for remote digital forensics, or perhaps any other task of your choice. It is meant to be transparent and monitorable by the owner of the system, forensically sound, customizable and compact.
- GetData Forensic Imager - GetData Forensic Imager is a Windows based program that will acquire, convert, or verify a forensic image in one of the following common forensic file formats.
- Guymager - Guymager is a free forensic imager for media acquisition on Linux.
- Magnet ACQUIRE - ACQUIRE by Magnet Forensics allows various types of disk acquisitions to be performed on Windows, Linux, and OS X as well as mobile operating systems.

Evidence Collection Tools

- Bulk*extractor* - bulkextractor is a computer forensics tool that scans a disk image, a file, or a directory of files and extracts useful information without parsing the file system or file system structures. Because of ignoring the file system structure, the program distinguishes itself in terms of speed and thoroughness.
- Cold Disk Quick Response - uses a streamlined list of parsers to quickly analyze a forenisic image file, dd, E01, .vmdk, etc, and output nine reports.
- Ir-rescue - -ir-rescue - is a Windows Batch script and a Unix Bash script to comprehensively collect host forensic data during incident response.

- Live Response Collection - The Live Response collection by BriMor Labs is an automated tool that collects volatile data from Windows, OSX, and -nix based operating systems.

Incident Management Tools

- Cortex XSOAR - Security orchestration tool. Formerly Demisto community edition. Offers full Incident lifecycle management, Incident Closure Reports, team assignments and collaboration, and many integrations to enhance automations, like Active Directory, PagerDuty, Jira and much more.
- CyberCPR - A community and commercial incident management tool with Need-to-Know built in to support GDPR compliance while handling sensitive incidents.
- Cyphon - Cyphon eliminates the headaches of incident management by streamlining a multitude of related tasks through a single platform. It receives, processes and triages events to provide an all-encompassing solution for your analytic workflow — aggregating data, bundling and prioritizing alerts, and empowering analysts to investigate and document incidents.
- FIR - Fast Incident Response, FIR, is an cybersecurity incident management platform designed with agility and speed in mind. It allows for easy creation, tracking, and reporting of cybersecurity incidents and is useful for CSIRTs, CERTs and SOCs alike.
- RTIR - Request Tracker for Incident Response, RTIR, is the premier open source incident handling system targeted for computer security teams. We worked with over a dozen CERT and CSIRT teams around the world to help you handle the ever-increasing volume of incident reports. RTIR builds on all the features of Request Tracker.
- SCOT - Sandia Cyber Omni Tracker, SCOT, is an Incident Response collaboration and knowledge capture tool focused on flexibility and ease of use. Our goal is to add value to the incident response process without burdening the user.
- Threat_note - A lightweight investigation notebook that allows security researchers the ability to register and retrieve indicators related to their research.

Linux Forensics Distributions

- ADIA - The Appliance for Digital Investigation and Analysis, ADIA, is a VMware-based appliance used for digital investigation and acquisition and is built entirely from public domain software. Among the tools contained in ADIA are Autopsy, the Sleuth Kit, the Digital Forensics Framework, log2timeline, Xplico, and Wireshark. Most of the system maintenance uses Webmin. It is designed for small-to-medium sized digital investigations and acquisitions. The appliance runs under Linux, Windows, and Mac OS. Both i386 32-bit and x86_64 versions are available.
- CAINE - The Computer Aided Investigative Environment, CAINE, contains numerous tools that help investigators during their analysis, including forensic evidence collection.
- CCF-VM - CyLR CDQR Forensics Virtual Machine, CCF-VM: An all-in-one solution to parsing collected data, making it easily searchable with built-in common searches, enable searching of single and multiple hosts simultaneously.
- DEFT - The Digital Evidence & Forensics Toolkit, DEFT, is a Linux distribution made for computer forensic evidence collection. It comes bundled with the Digital Advanced Response Toolkit, DART, for Windows. A light version of DEFT,

called DEFT Zero, is also available, which is focused primarily on forensically sound evidence collection.
- NST - Network Security Toolkit - Linux distribution that includes a vast collection of best-of-breed open source network security applications useful to the network security professional.
- PALADIN - PALADIN is a modified Linux distribution to perform various forenics task in a forensically sound manner. It comes with many open source forensics tools included.
- Security Onion - Security Onion is a special Linux distro aimed at network security monitoring featuring advanced analysis tools.
- SIFT Workstation - The SANS Investigative Forensic Toolkit, SIFT, Workstation demonstrates that advanced incident response capabilities and deep dive digital forensic techniques to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

Linux Evidence Collection

- FastIR Collector Linux - FastIR for Linux collects different artefacts on live Linux and records the results in csv files.

Log Analysis Tools

- Logdissect - A CLI utility and Python API for analyzing log files and other data.
- Lorg - a tool for advanced HTTPD logfile security analysis and forensics.

OSX Evidence Collection

- Knockknock - Displays persistent items, scripts, commands, binaries, etc., that are set to execute automatically on OSX.
- Mac_apt - macOS Artifact Parsing Tool - Plugin based forensics framework for quick mac triage that works on live machines, disk images or individual artifact files.
- OSX Auditor - OSX Auditor is a free Mac OS X computer forensics tool.
- OSX Collector - An OSX Auditor offshoot for live response.

Incident Response Playbooks

- IR Workflow Gallery - Different generic incident response workflows, e.g. for malware outbreak, data theft, unauthorized access,... Every workflow constists of seven steps: prepare, detect, analyze, contain, eradicate, recover, post-incident handling.
- IRM - Incident Response Methodologies by CERT Societe Generale.
- PagerDuty Incident Response Documentation - Documents that describe parts of the PagerDuty Incident Response process. It provides information not only on preparing for an incident, but also what to do during and after.

Process Dump Tools

- Microsoft User Mode Process Dumping - User mode process dumping guide.
- PMDump - PMDump is a tool that lets you dump the memory contents of a process to a file without stopping the process.

Sandboxing/reversing tools

- Cuckoo - Open Source Highly configurable sandboxing tool.
- Cuckoo-modified - Heavily modified Cuckoo fork developed by community.
- Cuckoo-modified-api - A Python library to control a cuckoo-modified sandbox.
- Hybrid-Analysis - Hybrid-Analysis is a free powerful online sandbox by Payload Security.
- Malwr - Malwr is a free online malware analysis service and community, which is powered by the Cuckoo Sandbox.
- Mastiff - MASTIFF is a static analysis framework that automates the process of extracting key characteristics from a number of different file formats.
- Metadefender Cloud - Metadefender is a free threat intelligence platform providing multiscanning, data sanitization and vulnerability assesment of files.
- Viper - Viper is a python based binary analysis and management framework, that works well with Cuckoo and YARA
- Virustotal - Virustotal, a subsidiary of Google, is a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners.
- Visualize_Logs - Open source. Visualization library and command line tools for logs.

Timeline tools

- Highlighter - Free Tool available from Fire/Mandiant that will depict log/text file that can highlight areas on the graphic, that corresponded to a key word or phrase. Good for time lining an infection and what was done post compromise.
- Morgue - A PHP Web app by Etsy for managing postmortems.
- Plaso - a Python-based backend engine for the tool log2timeline.
- Timesketch - open source tool for collaborative forensic timeline analysis.

Windows Evidence Collection

- AChoir - Achoir is a framework/scripting tool to standardize and simplify the process of scripting live acquisition utilities for Windows.
- Binaryforay - list of free tools for win forensics.
- Crowd Response - Crowd Response by CrowdStrike is a lightweight Windows console application designed to aid in the gathering of system information for incident response and security engagements. It features numerous modules and output formats.
- FastIR Collector - FastIR Collector is a tool that collects different artefacts on live Windows systems and records the results in csv files. With the analyses of these artefacts, an early compromise can be detected.
- FECT - Fast Evidence Collector Toolkit, FECT, is a light incident response toolkit to collect evidences on a suspicious Windows computer. Basically it is intended to be used by non-tech savvy people working with a journeyman Incident Handler.
- Fibratus - tool for exploration and tracing of the Windows kernel.
- IREC - All-in-one IR Evidence Collector which captures RAM Image, $MFT, EventLogs, WMI Scripts, Registry Hives, System Restore Points and much more. It is FREE, lightning fast and easy to use.
- IOC Finder - IOC Finder is a free tool from Mandiant for collecting host system data and reporting the presence of Indicators of Compromise. Support for Windows only.
- LOKI - Loki is a free IR scanner for scanning endpoint with yara rules and other indicators.

- Panorama - Fast incident overview on live Windows systems.
- PowerForensics - Live disk forensics platform, using PowerShell.
- PSRecon - PSRecon gathers data from a remote Windows host using PowerShell] (v2 or later), organizes the data into folders, hashes all extracted data, hashes PowerShell and various system properties, and sends the data off to the security team. The data can be pushed to a share, sent over email, or retained locally.
- RegRipper - Regripper is an open source tool, written in Perl, for extracting/parsing information, keys, values, and data from the Registry and presenting it for analysis.
- TRIAGE-IR - Triage-IR is a IR collector for Windows.

Other

- BruteX Wordlists - Wordlist repo.
- Cortex - Cortex allows you to analyze observables such as IP and email addresses, URLs, domain names, files or hashes one by one or in bulk mode using a Web interface. Analysts can also automate these operations using its REST API.
- Crits - a web-based tool which combines an analytic engine with a cyber threat database .
- Diffy - a DFIR tool developed by Netflix's SIRT that allows an investigator to quickly scope a compromise across cloud instances (Linux instances on AWS, currently) during an incident and efficiently triaging those instances for followup actions by showing differences against a baseline.
- domfind - domfind is a Python DNS crawler for finding identical domain names under different TLDs.
- Fenrir - Fenrir is a simple IOC scanner. It allows scanning any Linux/Unix/OSX system for IOCs in plain bash. Created by the creators of THOR and LOKI.
- Fileintel - Pull intelligence per file hash.
- fuzzbox - Multi-codec media fuzzing tool.
- Google Hacking Master List
- HELK - Threat Hunting platform.
- Hindsight - Internet history forensics for Google Chrome/Chromium.
- honggfuzz - Security orientated fuzzing tool.
- Hostintel - Pull intelligence per host.
- imagemounter - Command line utility and Python package to ease the (un)mounting of forensic disk images.
- Kansa - Kansa is a modular incident response framework in Powershell.
- Kayak Car Hacking Tool - Tool for Kayak car hacking.
- melkor-android - Android fuzzing tool for ELF file formats.
- Netzob - Multipurpose tool for reverse engineering, modeling, and fuzzing communciation protocols.
- radamsa - General purpose fuzzing tool.
- RaQet - RaQet is an unconventional remote acquisition and triaging tool that allows triage a disk of a remote computer (client) that is restarted with a purposely built forensic operating system.
- rastrea2r - allows one to scan disks and memory for IOCs using YARA on Windows, Linux and OS X.
- ROPgadget - Python based tool to aid in ROP exploitation.
- Shellen - Interactive shellcoding environment.
- sqhunter - a threat hunter based on osquery and Salt Open (SaltStack) that can issue ad-hoc or distributed queries without the need for osquery's tls plugin.

sqhunter allows you to query open network sockets and check them against threat intelligence sources.
- Stalk - Collect forensic data about MySQL when problems occur.
- Stenographer - Stenographer is a packet capture solution which aims to quickly spool all packets to disk, then provide simple, fast access to subsets of those packets. It stores as much history as it possible, managing disk usage, and deleting when disk limits are hit. It's ideal for capturing the traffic just before and during an incident, without the need explicit need to store all of the network traffic.
- Sulley - Fuzzing engine and framework.
- traceroute-circl - traceroute-circl is an extended traceroute to support the activities of CSIRT (or CERT) operators. Usually CSIRT team have to handle incidents based on IP addresses received. Created by Computer Emergency Responce Center Luxembourg.
- Zulu - Interactive fuzzer.

Our Open Source Tools

- Legion - Legion is an open source, easy-to-use, super-extensible and semi-automated network penetration testing tool that aids in discovery, reconnaissance and exploitation of information systems.